ANGIER POLICE DEPARMTENT

STANDARD OPERATING PROCEDURES MANUAL

APD SECTION	TITLE	GENERAL ORDER
1	License Plate Readers	15
CHIEF SIGNATURE		DATE
Garland Lee Thompson, Jr.		

I. Purpose

A. The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology (N.C.G.S. § 20-183.31).

II. Policy

A. The policy of the Angier Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

B. All data and images gathered by the ALPR are for the official use of this department, and other recognized law enforcement agencies. The information garnered may contain confidential information, it is not open to public review.

III. Administration

A. The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Angier Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction, and stolen property recovery.

B. All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Captain. The Administration Captain will assign members under the Administration Captain's command to administer the day-to-day operation of the ALPR equipment and data.

IV. Operations

A. Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

1. An ALPR shall only be used for official law enforcement business.

2. An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

3. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings, and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

4. No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

5. No ALPR operator may access confidential department, state or federal data unless authorized to do so.

6. If practicable, the officer should verify an ALPR response through the Division of Criminal Investigation Network (DCIN) before taking enforcement action that is based solely on an ALPR alert (N.C.G.S. § 20-183.31).

7. ALPR data shall not be used for the enforcement of traffic violations (N.C.G.S. § 20-183.31).

B. Supervisor Responsibilities

1. Supervisors should appropriately monitor ALPR operators to ensure that use of the ALPR equipment and data is consistent with this policy (N.C.G.S. § 20-183.31). Any use of the ALPR system that violates the restrictions contained in this policy may result in disciplinary action.

V. Data Retention and Collection

A. The Chief of Police or his designee is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with the programming of the systems and department policy.

B. All stored ALPR data should be retained in accordance with the established records retention schedule. Thereafter, ALPR data shall be purged after 30 days unless a warrant has been issued for the data or it is subject to a written and sworn retention request submitted pursuant to N.C.G.S. § 20-183.32.

C. Data being retained pursuant to a retention request should be downloaded onto portable media, booked into evidence, and retained for a period of one year after the initial request unless a subsequent request to maintain the data is received (N.C.G.S. § 20-183.32)

VI. Accountability

A. All data will be closely safeguarded and protected by both procedural and technological means. The Angier Police Department will observe the following safeguards regarding access to and use of stored data:

1. All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

2. Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

3. ALPR system audits should be conducted on a regular basis.

VII. System Integrity

A. The Chief of Police or his designee shall maintain a schedule to regularly perform audits, maintenance checks and any needed corrections or adjustments to the ALPR system. The audits shall be conducted at least annually and include a report on the use and effectiveness of the system (N.C.G.S. § 20-183.31).

B. The ALPR system should be updated every 24 hours or as soon as practicable thereafter with any license plate data obtained from the DCI network or any other databases used in conjunction with the ALPR system (N.C.G.S. § 20-183.32).

VIII. Releasing ALPR Data

A. ALPR data shall only be shared with another law enforcement agency or prosecutor upon a written request, which may be made electronically. The release of ALPR data is not required if the disclosure of requested ALPR data will compromise an on-going investigation (N.C.G.S. § 20-183.32).

B. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

IX. Requests to Outside Agencies

A. Members requesting the retention or release of ALPR data maintained by another agency should obtain supervisory approval prior to making the request. Members may request the disclosure of data from another agency by submitting a request in writing. Members requesting that data be retained by another agency must submit a sworn written statement as required by N.C.G.S. § 20-183.32. A copy of any requests shall be retained in a case file.

B. Efforts should be made as soon as practicable to obtain a search warrant to access requested data. The member requesting the data should contact the outside agency to cancel any request should the information no longer be needed (N.C.G.S. § 20-183.31).

X. Training

A. Subject to available resources, the Department should provide periodic training on the use and operation of the ALPR equipment, the collection of ALPR data and the security and release of ALPR data (N.C.G.S. § 20-183.31).

B. No member is allowed the use of the ALPR mobile systems until training on the use, operation and retention of the ALPR equipment, collection of ALPR data and the security and release of ALPR data and documentation has been provided to the Major. (N.C.G.S. 20-183.31)

XI. Use of ALPR by Outside Agencies.

A. The use of the ALPR systems and technologies is allowed at the discretion of the Chief of Police or his designee. A written request of dates and times of use shall be submitted at least seventy-two hours prior to date of use, or as soon as practicable thereafter and can be submitted electronically to the Chief of Police.

B. The Chief of Police or his designee shall keep records of the dates and times used as provided in the Records Maintenance and Release Policy.

C. Any agency requesting the use of the ALPR systems and technology shall attend training provided by the Town of Angier or training offered by the company that the ALPR systems and technology is manufactured by.

D. Documentation of the training shall by submitted with the initial request and shall be kept on file for posteriority.

XII. Development of a Hot List

A Hot list is created because a license plate associated with a vehicle of interest from NCIC or a vehicle involved in a criminal investigation.

A. Hot Lists will primarily be compiled from vehicles associated with NCIC entries for the following categories.

1. Stolen Vehicles

2. Gang or Suspected Terrorists

3. Missing Persons

4. Stolen License Plates

5. Wanted Persons Warrant Entered into NCIC

B. Hot Lists may also include vehicles from any of the following categories:

1. Homicides

2. Aggravated Assaults/Sexual Assaults

3. Robbery

4. Burglary or Break-ins

5. Amber Alert/ Silver Alert/ Blue Alert

6. Involuntary Commitment Orders/ Mental patient currently in crisis

7. Stolen Property

8. Hit and Run Vehicle

9. Vehicles that fled from a traffic stop

10. Requests for assistance from other agencies

11. Narcotic Investigations

12. Investigations approved by the officer's supervisor

C. Hot Lists SHALL NOT include license plate associated with regulatory motor vehicle violations (i.e. expired registration, inspection violations, driver's license violations)

XIII. Program Oversight/ Evaluation/ Audit Review

A. All requests for shared data access from other law enforcement agencies and/or invitations to access data from private ALPR systems (i.e. HOA's, Community Watch Groups) shall be forwarded to the Chief of Police for approval.

B. Damage or other malfunctions to the equipment will be reported to the officer's immediate supervisor.

C. All successful uses of the ALPR shall be documented and forwarded to the ALPR program supervisor.

D. The supervisor of the ALPR program will be responsible for conducting, reviewing and retaining audits of the ALPR system. These audits shall be forwarded through the chain of command to the Chief of Police annually. The audit information should include the following:

1. Records of ALPR operators and their ALPR usage, including vehicles of interest added to a hot list by individual officers.

2. A listing of access to the department's server, to include, additions and/or searches of the scan file, in order to verify security of that data and compliance with this policy.

3. Auditing the local hot lists to ensure manual entries are being deleted when no longer of interest.

5. Anyone becoming aware of a possible violation of this policy, including but not limited to the unauthorized access, use, release and/or dissemination of ALPR data, shall refer the matter to their supervisor